UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,537	02/09/2004	Brian Hernacki	SYMAP041	6706

21912 7590 07/31/2007
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
DEICHMEISTER, NICHOLAS F	
ART UNIT	**PAPER NUMBER**
2616	

MAIL DATE	DELIVERY MODE
07/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/775,537	HERNACKI, BRIAN	
	Examiner	Art Unit	
	Nick Deichmeister	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1 and 20-21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the corresponding data" in lines 6-7. There is insufficient antecedent basis for this limitation in the claim.

Claim 20 recites the limitation "the corresponding data" in line 18. There is insufficient antecedent basis for this limitation in the claim.

Claim 21 recites the limitation "the corresponding data" in lines 6-7. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1 and 20-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Malagrino et al (U.S. Patent No. 6,714,985 B1).

Malagrino et al discloses a method and apparatus for efficiently reassembling fragments received at an intermediate station in a computer network, comprising the following features:

Regarding claim 1, a method for assembling fragmented network traffic (col. 3, lines 29-32, reassembly of IP fragments received at an intermediate station in a computer network), comprising: detecting (col. 7, lines 20-21, analyzes the fragments to counter attacks) in the fragmented network traffic (col. 7, line 20, fragments) an anomaly (col. 7, line 20, attacks) that could result in two or more fragments comprising the fragmented network traffic (col. 10, line 35, all fragments belonging to the particular packet) being reassembled (col. 10, lines 35-36, packet that is to be reassembled) at a monitoring node (col. 12, lines 9-10, intermediate station) to obtain a reassembled data flow (col. 11, lines 59-60, reassembly process can take place) that is different than the corresponding data as reassembled at a destination node (col. 11, line 59-col. 12, line 11, approach described herein for computing the offset of the next fragment is not typically used to reassemble fragments according to the IP reassembly process; IP reassembly usually takes place in host stations as opposed to intermediate stations)... ***The examiner notes that applicant discloses the possibility that the configuration of the host receiving fragments may affect the way in which the said fragments are reassembled (see specification, pp. 7, lines 4-11).**

...to which the fragmented network traffic is addressed (col. 11, line 67-col. 12, line 1, host stations); and performing further processing on the fragmented network traffic having the anomaly (col. 7, line 20, counter attacks; col. 7, lines 24-26, typically, a switch that is configured to perform such higher layer functions implements the IP reassembly processing in software).

Regarding claim 20, a system for assembling fragmented network traffic (col. 3, lines 29-32, reassembly of IP fragments received at an intermediate station in a computer network), comprising: a memory (col. 11, line 40 frame buffer) configured to store at least a portion of the fragmented network traffic (col. 11, lines 39-40, fragment/packet information stored in the frame buffer); and a processor (fig. 4, main controller 500) configured to detect (col. 7, lines 20-21, analyzes the fragments to counter attacks) in the fragmented network traffic (col. 7, line 20, fragments) an anomaly (col. 7, line 20, attacks) that could result in two or more fragments comprising the fragmented network traffic (col. 10, line 35, all fragments belonging to the particular packet) being reassembled (col. 10, lines 35-36, packet that is to be reassembled) at a monitoring node (col. 12, lines 9-10, intermediate station) to obtain a reassembled data flow (col. 11, lines 59-60, reassembly process can take place) that is different than the corresponding data as reassembled at a destination node (col. 11, line 59-col. 12, line 11, approach described herein for computing the offset of the next fragment is not typically used to reassemble fragments according to the IP reassembly process; IP reassembly usually takes place in host stations as opposed to intermediate stations)...

*****The examiner notes that applicant discloses the possibility that the configuration of the host receiving fragments may affect the way in which the said fragments are reassembled (see specification, pp. 7, lines 4-11).**

...to which the fragmented network traffic is addressed (col. 11, line 67-col. 12, line 1, host stations); and perform further processing on the fragmented network traffic having the anomaly (col. 7, line 20, counter attacks; col. 7, lines 24-26, typically, a switch that is configured to perform such higher layer functions implements the IP reassembly processing in software).

Regarding claim 21, a computer program product for assembling fragmented network traffic (col. 5, lines 23-25, software programs associated with the invention; col. 3, lines 29-32, reassembly of IP fragments received at an intermediate station in a computer network), the computer program product being embodied in a computer readable medium (col. 5, lines 21-25, storage locations addressable by the processor and adapter for storing software programs associated with the invention) and comprising computer instructions (col. 5, lines 23-25, software programs associated with the invention) for: detecting (col. 7, lines 20-21, analyzes the fragments to counter attacks) in the fragmented network traffic (col. 7, line 20, fragments) an anomaly (col. 7, line 20, attacks) that could result in two or more fragments comprising the fragmented network traffic (col. 10, line 35, all fragments belonging to the particular packet) being reassembled (col. 10, lines 35-36, packet that is to be reassembled) at a monitoring node (col. 12, lines 9-10, intermediate station) to obtain a reassembled data flow (col. 11, lines 59-60, reassembly process can take place) that is different than the

corresponding data as reassembled at a destination node (col. 11, line 59-col. 12, line 11, approach described herein for computing the offset of the next fragment is not typically used to reassemble fragments according to the IP reassembly process; IP reassembly usually takes place in host stations as opposed to intermediate stations)... *****The examiner notes that applicant discloses the possibility that the configuration of the host receiving fragments may affect the way in which the said fragments are reassembled (see specification, pp. 7, lines 4-11)** ...to which the fragmented network traffic is addressed (col. 11, line 67-col. 12, line 1, host stations); and performing further processing on the fragmented network traffic having the anomaly (col. 7, line 20, counter attacks; col. 7, lines 24-26, typically, a switch that is configured to perform such higher layer functions implements the IP reassembly processing in software).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malagrino et al in view of Pochon et al (U.S. Patent Application Publication No. 2003/0048793 A1).

Malagrino et al describes the claimed limitations as discussed in paragraph 4 above. Malagrino et al does not disclose the following features:

Regarding claim 2, wherein detecting an anomaly comprises determining that said two or more fragments overlap.

Regarding claim 3, wherein determining that said two or more fragments overlap comprises reading a header value associated with one of the fragments.

Regarding claim 4, wherein the header value comprises an offset value.

Regarding claim 5, wherein detecting an anomaly comprises determining that said two or more fragments overlap and that at least two of said fragments comprise different data for an overlapping portion of said fragments.

Regarding claim 6, wherein performing further processing comprises determining configuration information associated with said destination node.

Regarding claim 7, wherein determining configuration information comprises querying the destination node.

Regarding claim 8, wherein determining configuration information comprises querying an information base.

Regarding claim 9, wherein performing further processing comprises reassembling the fragmented network traffic to generate more than one variant of the reassembled data flow.

Regarding claim 10, further including processing the anomaly to determine whether the fragmented network traffic is associated with a threat.

Regarding claim 11, further including performing an action on the fragmented network traffic base don whether the fragmented network traffic is associated with a threat.

Regarding claim 12, further including discarding at least a portion of the fragmented network traffic if the fragmented network traffic is associated with a threat.

Regarding claim 13, further including copying one or more fragments comprising the fragmented network traffic to a buffer.

Regarding claim 14, wherein performing further processing comprises sending an alert.

Regarding claim 15, wherein performing further processing comprises determining whether the fragmented network traffic should be blocked.

Regarding claim 16, wherein performing further processing comprises determining whether the fragmented network traffic should be forwarded to the destination node.

Regarding claim 17, wherein performing further processing comprises determining whether to initiate increased buffering of the fragmented network traffic.

Regarding claim 18, wherein performing further processing comprises initiating increased buffering of the fragmented network traffic if it is determined that two or more fragments comprising said fragmented network traffic have overlapping portions.

Regarding claim 19, wherein performing further processing comprises initiating increased buffering of the fragmented network traffic if it is determined that two or more

fragments comprising said fragmented network traffic have mismatching overlapping portions.

Pochon et al discloses a method an apparatus for data normalization, comprising the following features:

Regarding claim 2, wherein detecting an anomaly comprises determining that said two or more fragments overlap (par. 0022, line 3, overlapping positions).

Regarding claim 3, wherein determining that said two or more fragments overlap comprises reading a header value (par. 0055, lines 1-2, header field FRAGMENT OFFSET) associated with one of the fragments (par. 0055, line 1, for each datagram).

Regarding claim 4, wherein the header value comprises an offset value (par. 0055, lines 1-2, FRAGMENT OFFSET).

Regarding claim 5, wherein detecting an anomaly comprises determining that said two or more fragments overlap (par. 0022, line 3, overlapping positions) and that at least two of said fragments comprise different data (fig. 3, fragment 1 and fragment 2; note that said fragments contain different information) for an overlapping portion (par. 0022, line 3, overlapping positions) of said fragments.

Regarding claim 6, wherein performing further processing comprises determining configuration information (par. 0103, lines 4-6, traffic normalizer tries to obtain the required data or discards the received datagram or fragment if the addressed end-system does not respond) associated with said destination node (par. 0103, line 6, end-system).

Regarding claim 7, wherein determining configuration information comprises querying the destination node (par. 0103, lines 4-6, traffic normalizer tries to obtain the required data or discards the received datagram or fragment if the addressed end-system does not respond).

Regarding claim 8, wherein determining configuration information comprises querying an information base (par. 0103, line 3, stored in the normalization table).

Regarding claim 9, wherein performing further processing comprises reassembling the fragmented network traffic (fig. 4, reassembled datagram(s)) to generate more than one variant (fig. 4, reassembled datagram near host A is different from reassembled datagram near NIDS) of the reassembled data flow.

Regarding claim 10, further including processing (par. 0050, lines 1-2, normalization of traffic data) the anomaly to determine (par. 0050, lines 2-3, network intrusion detection system) whether the fragmented network traffic is associated with a threat (par. 0050, lines 2-3, network intrusion detection system).

Regarding claim 11, further including performing an action (par. 0052, lines 4-5, discarding or redirecting) on the fragmented network traffic (par. 0052, line 4, fragments) based on whether the fragmented network traffic is associated with a threat (par. 0050, lines 2-3, network intrusion detection system).

Regarding claim 12, further including discarding (par. 0052, lines 4-5, discarding) at least a portion (par. 0052, line 1, fragments) of the fragmented network traffic if the fragmented network traffic is associated with a threat (par. 0050, lines 2-3, network intrusion detection system).

Regarding claim 13, further including copying one or more fragments comprising the fragmented network traffic (par. 0054, lines 3-4, payload or data of data packets or fragments is transiently stored) to a buffer (par. 0054, line 4, stored).

Regarding claim 14, wherein performing further processing comprises sending an alert (par. 0027, lines 9-10, sends an error message back to the source).

Regarding claim 15, wherein performing further processing comprises determining whether the fragmented network traffic should be blocked (abstract, lines 10-12, packets of data such as IP datagrams are modified, redirected or **discarded**).

Regarding claim 16, wherein performing further processing comprises determining whether the fragmented network traffic should be forwarded to the destination node (abstract, lines 1-5, traffic data that is simultaneously transferred to a network intrusion detection system and **monitored end-systems**).

Regarding claim 17, wherein performing further processing comprises determining whether to initiate increased buffering (par. 0040, line 8, use up memory space) of the fragmented network traffic.

Regarding claim 18, wherein performing further processing comprises initiating increased buffering (par. 0040, line 8, use up memory space) of the fragmented network traffic if it is determined that two or more fragments comprising said fragmented network traffic have overlapping portions (fig. 4, overlap of fragments 1 and 2).

Regarding claim 19, wherein performing further processing comprises initiating increased buffering (par. 0040, line 8, use up memory space) of the fragmented network

traffic if it is determined that two or more fragments comprising said fragmented network traffic have mismatching overlapping portions (fig. 4, overlap of fragments 1 and 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Malagrino et al by using the features, as taught by Pochon et al, in order to provide reduced susceptibility to congestion or vulnerability to denial of service attacks (Pochon et al, par. 0054, lines 5-7).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Rose et al (U.S. Patent Application Publication No. 2004/0205228 A1) discloses an apparatus and method for detecting tiny fragment attacks. Kaler et al (U.S. Patent Application Publication No. 2004/0003286 A1) discloses distributed threat management. Fink et al (U.S. Patent No 6,496,935 B1) discloses a system, device and method for rapid packet filtering and processing. Singh et al (U.S. Patent Application Publication No. 2006/0098585 A1) discloses detecting malicious attacks using network behavior and header analysis. Neale et al (U.S. Patent No. 6,975,647 B2) discloses enhancements for TCP performance enhancing proxies.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nick Deichmeister whose telephone number is (571) 272-9746. The examiner can normally be reached on Monday through Friday (off alternate Fridays).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kwang Yao can be reached on (571) 272-3182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NFD

KWANG BIN YAO
SUPERVISORY PATENT EXAMINER